DEPART

Office of Justice Programs

[OMB Number 1121-NEW]

Agency Information Collection Activities; Proposed eCollection eComments Requested

AGENCY: Bureau of Justice Statistics, Office of Justice Programs, Department of Justice.

ACTION: 60 Day Notice.

SUMMARY: The Department of Justice, Office of Justice Programs, Bureau of Justice Statistics is submitting the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995.

DATES: The Department of Justice encourages public comment and will accept input until [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]

FOR FURTHER INFORMATION CONTACT: If you have additional comments especially on the estimated public burden or associated response time, suggestions, or additional information, please contact the Bureau of Justice Statistics, 810 Seventh Street NW, Washington, DC 20531; telephone (202) 307-0765 or send an email to askbjs@usdoj.gov. Please include "STANDARD APPLICATION PROCESS" in the subject line.

SUPPLEMENTARY INFORMATION: Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address one or more of the following four points:

- Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Bureau of Justice Statistics, including whether the information will have practical utility;
- Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information;
- Evaluate whether and if so how the quality, utility, and clarity of the information to be collected can be enhanced; and
- Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

OVERVIEW OF THIS INFORMATION COLLECTION:

1. *Type of Information Collection:* Request for access
2. *The Title of the Form/Collection:* Data Security Requirements for Accessing Confidential Data
3. *The agency form number, if any, and the applicable component of the Department of Justice sponsoring the collection:* There is no form number associated with this information collection. The applicable component within the Department of Justice is the Bureau of Justice Statistics (BJS), in the Office of Justice Programs.
4. *Affected public who will be asked or required to respond, as well as a brief abstract:* The Foundations for Evidence-Based Policymaking Act of 2018 mandates that the OMB establish a Standard Application Process (SAP) for requesting access to certain confidential data assets for statistical purposes, including evidence-building The SAP is to be a process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply to access

confidential data assets held by a federal statistical agency or unit for the purposes of developing evidence. With the Interagency Council on Statistical Policy (ICSP) as advisors, the entities upon whom this requirement is levied are working with the SAP Project Management Office (PMO) and with OMB to implement the SAP. The SAP Portal is to be a single web-based common application for requesting access to confidential data assets from federal statistical agencies and units. On behalf of BJS and the other federal statistical agencies and units, the National Center for Science and Engineering Statistics (NCSES) submitted a Federal Register Notice in September 2022 announcing plans to collect information through the SAP Portal (87 FR 53793).

Once an application for confidential data is approved through the SAP Portal, BJS will collect information to meet its data security requirements when providing access to restricted use (confidential) microdata for the purpose of evidence building. This collection will occur outside of the SAP Portal. BJS's data security agreements and other paperwork along with the corresponding security protocols allow the agency to maintain careful controls on confidentiality and privacy, as required by law. If an application requesting access to an BJS-owned confidential data asset is approved, BJS will contact the applicant(s) to initiate the process of collecting the following information to fulfill its data security requirements:

- **Restricted data use agreement** – This document is an agreement between BJS's official archive (currently the National Archive of Criminal Justice Data [NACJD]), on behalf of BJS, and the user(s) who is approved to access BJS's confidential data assets exclusively for statistical purposes, including evidence-building, in accordance with the terms and conditions stated in the agreement and all applicable federal laws and regulations. An applicant must submit the appropriate data security plan information to describe how they

will protect the data from misuse and unauthorized access. The agreement describes the penalties associated with the misuse or unauthorized access of the data. The agreement requires signature from the applicant(s) and any other representative who has the authority to enter into a legal agreement with NACJD, as applicable.

- **Privacy Certificate** – Office of Justice Programs regulations at 28 C.F.R. Part 22 require that a Privacy Certificate be submitted as part of any application for a project in which information identifiable to a private person will be collected, analyzed, or otherwise used for research or statistical purposes. The Privacy Certificate describes the specific technical, administrative, and physical controls and procedures that will be used to protect data confidentiality and safeguard the data from misuse or unauthorized access. The Privacy Certificate is an applicant's certification to comply with BJS's confidentiality requirements. All individuals who will have access to the confidential BJS data are required to sign a Privacy Certificate to affirm their understanding of and agreement to comply with BJS's confidentiality requirements.
- **Data security plan** – This document describes the data access modality requested (physical enclave, virtual enclave, or secure download) and the specific data security measures and technical, physical, and administrative controls that will be followed to protect data from unauthorized disclosure and misuse.
- **Confidentiality pledge** – This document describes the applicant's responsibilities related to accessing restricted data and confidentiality protections the applicant(s) must uphold, including adhering to applicable federal laws and regulations. The assurance requires signature from the

applicant(s) and certifies their understanding of and agreement to fulfill the terms in the data use agreement and data security plan.

- **Institutional Review Board (IRB) documentation** – Users of BJS restricted data must comply with Department of Justice regulations at 28 C.F.R. Part 46 (Protection of Human Subjects), including ensuring that adequate protections are in place to protect the confidentiality of information identifiable to a private person. Applicants must submit the appropriate documentation to demonstrate that an IRB has approved or exempted the proposed project using BJS restricted data in accordance with the requirements in 28 C.F.R. Part 46.
- **Certification of training** – Users of BJS restricted data will be required to complete relevant data security, confidentiality, and privacy training, as appropriate, and provide written certification of completion.

5. *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* The amount of time to complete the agreements and other paperwork that comprise BJS's security requirements will vary based on the confidential data assets requested. To obtain access to BJS confidential data assets, it is estimated that the average time to complete and submit BJS's data security agreements, IRB application, and other paperwork is 3 hours (180 minutes). This estimate does not include the time needed to complete and submit an application within the SAP Portal or time waiting to receive a decision from an IRB determination after submitting an application. All efforts related to SAP Portal applications occur prior to and separate from BJS's effort to collect information related to data security requirements.
6. *An estimate of the total public burden (in hours) associated with the collection:* The expected number of applications in the SAP Portal that receive a positive determination from BJS in a given year may vary. Overall, per year, BJS

estimates it will collect data security information for 55 application submissions that received a positive determination within the SAP Portal. BJS estimates that the total burden for the collection of information for data security requirements over the course of the three-year OMB clearance will be about 495 hours and, as a result, an average annual burden of 165 hours.

If additional information is required contact: Robert Houser, Department Clearance Officer, Policy and Planning Staff, Justice Management Division, United States Department of Justice, Two Constitution Square, 145 N Street NE, 3E.206, Washington, DC 20530.

Dated: November 14, 2022.

Robert Houser,

Department Clearance Officer for PRA,

Policy and Planning Staff,

Office of the Chief Information Officer,

U.S. Department of Justice.

Billing Code: 4410-18

[FR Doc. 2022-25036 Filed: 11/16/2022 8:45 am; Publication Date: 11/17/2022]